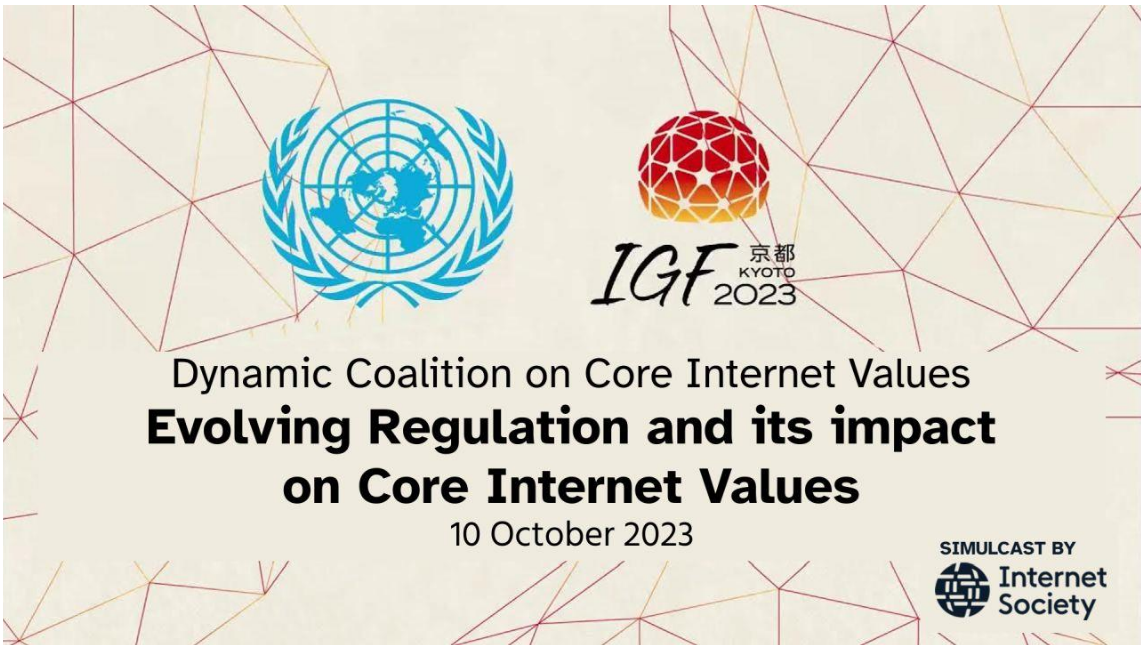
IGF 京都 KYOTO 2023
Dynamic Coalition on Core Internet Values
Evolving Regulation and its impact on Core Internet Values
10 October 2023
SIMULCAST BY
Internet Society

IGF

Dynamic Coalition on Core Internet Values (DC-CIV)

Evolving Regulation and its impact on Core Internet Values

Internet Governance Forum, Kyoto, Japan

Sébastien Bachollet: …build and evolve and derive universal values that emerge from the way the Internet works. The Internet is a global medium open to all, regardless of geography or nationality. It's interoperable because it's a network of networks. It doesn't rely on a single application. It relies on open protocols such as TCPIP and BGP.

It's free. of any centralized control, except for the needed coordination of unique identifiers. It's end to end, so traffic from one end of the network to the other end of the network goes. It's user centric and users have control over what they send and receive and it's robust and reliable.

So, the Dynamic Coalition on Core Internet Values held sessions at every previous IGF. And every year there seems to be another challenge, one of the most basic core Internet value, its unique weakness. In 2023, the world economy having not recovered from the challenge of previous years. What was free on the Internet might no longer make sense financially for companies offering the service, and might end up behind a paywall, what was free movement of information in the past might not be seen by government as a good thing today. What was free connectivity might not be financially sustainable any longer. What was free might be blocked tomorrow for many reasons. On the one hand, there are calls for commercial operators, such as telecom providers, asking for a fair share of Internet profits, which is gaining ground with some lawmakers.

In addition to this commercial pressure, where the free mode of operation might no longer be the preferred mode of operation, recent years have seen a lot more regulation affecting the Internet. Whether it is the UK's Online Safety Bill, the Australian Online Safety Act, The European Digital Services Act and Digital Market Act or the U. S. Kids, sorry, Online Safety Acts regulation is being drafted and ruled out by many governments, very often for good reason and good objective, but it's something we will see during this discussion. So not only is there a strong movement worldwide to implement some major structural change to the way the Internet and Internet services work, there is also a commercial interest from some to change the Internet business model altogether.

A few years ago, the Dynamic Coalition on Core Internet Value promoted permissionless innovation. These days, for many governments, this translates to the World Wild West. Is this a fair assessment of the Internet that we have been defending? Are the core values that gave Internet its freedom at risk?

Regulation, it's now firmly back on the agenda.

This session of the Dynamic Coalition on Core Internet Values will again bring world class experts to discuss the Internet we want, each bringing their unique experience to the table. I will briefly talk about our speaker. We are Here on my right, Lee Rainey.

I will leave them to present themselves. It will be shorter. Jane Coffin is with us. Nii Quaynor and Iria Puyosa are online. And Vint Cerf is with us. I would like to thank them very much. And give the floor if you agree, to Lee to start the discussion. Lee, the floor is yours.

Lee Rainie: Thank you, Sebastian.

It's wonderful to be here. I'm honored to be here and really, my philosophy has been whenever you're in the same room with Vint, sir, if you have to start by saying thank you and I come to you from 24 years of doing research with the Pew Research Center about the social and political and economic impacts of the Internet.

I thought I was going to retire. Thank you, sir.

And I flunked retirement, so I I got a wonderful gig to continue on with a portion of the work at Elon University, which is in North Carolina, United States. We've done a lot of work with them related to that. And I get the title Professor in front of my main name now. So my mother is smiling at me in heaven, and my children laugh at me a little bit less now.

I wanted to start by saying this overlying topic here is fragmentation. And so the first thing maybe to note in the sense of fragmentation is that there are 2.6 billion people who don't have the Internet and don't use it. And so there is a, an enormous fragmentation at the heart of the social, political, cultural experience of the Internet.

So I, just noting that is an important scene setter for this conversation. Over the course of my work at Pew, though it was easy to spot four different revolutions that were occurring on our watch and watch then the the reckoning that came from those revolutions. There was a dynamic that has tightened up.

There, there's usually great enthusiasm at that moment. Zero, and then the enthusiasm sometimes faded as the reality of things came out. So I want to also make sure that you understand, I'm going to be talking about for social, cultural and legal changes. These don't really affect. The IXP can affect how people think about the underlying principles of the Internet, they love it, you pull on the ideas of a free, open, secure, interoperable and you you get unprecedentedly positive.

survey ratings about the principles that underlie what the master here built. What happens though is that once those principles collide with culture and law and people's own personalities, there are ways in which their enthusiasms begin to fade or their qualms begin to rise. So go through the four revolutions relatively quickly.

The first one we saw in the late 1990s, beginning in the late 1990s, was the rise of home broadband, which made people enthusiastic users of Internet protocols because the Internet became a utility in their life. It was not a play thing anymore, as when you dialed up those modems, that was a fun sound to hear.

But when it became always on and on higher speed, people began to embrace it in the rhythms of their life. It changed the volume of information that was coming into their life, and it was, you could see the incipient ways that they became enthusiastic about being content creators themselves. So it was democratizing.

It was and doing end runs around gatekeepers. There were ways in which new kinds of communities could be built that were built around affinity and affiliation rather than localities and the physical proximity that people had to each other. And people just love the idea that they could tell their stories without being shut down or without having to cajole a gatekeeper to allow them to tell their stories.

And yet, right in those early days, there were early signs that people, while they liked that for themselves, they didn't like that necessarily for others who had different ideas. The medical community at first was one of the, was one of the initial communities to sound alarms around mis and disinformation.

They were worried from a gatekeeper sense that people were doing end rounds or end runs around their providers and getting second opinions and diagnosing themselves and things. But there was also concern that more and more misinformation and bad, just bad information was getting out into the world.

Dangerous actors early on. began to figure out how to exploit these new tools for themselves. Concern about the content that was appropriate for, particularly for children, to be exposed to. I came out of the world of journalism too, so it was easy to see the warning signs of what the Internet was going to be doing to mainstream journalism in the culture.

So that was part of the backlash. Love at first, democratizing, but also concerns about some of the early... Ways in which it was playing through the culture. Second revolution was the mobile connectivity revolution, which changed the velocity of information into people's lives. All of a sudden, their phones became another body part and another lobe in their brain.

And they loved that. They loved the always on, always available connectivity that they have with others. They like being able to be reached by others. They like the, this the fact that they... the nature of their social networks was changing even before social media really came to prominence.

They just could see more people in their lives and interact with more people and they enjoyed that. But they, again, early enough in that whole arrival of that second revolution on mobile connectivity, they began to worry about the distractions. that it was bringing into people's lives, the way it was disrupting their attention flows, the way that they were always available to others.

They liked it in some sense, they certainly liked it when they could do outreach to others, but they didn't like necessarily being always available to others. And it imposed new obligations on their lives. So again, there's this sort of push me, pull you, yin and yang dimension to the rise of, of this second revolution.

Third revolution is social media. In particularly when combined with the mobile connectivity revolution, it just put everything on accelerants. Their relationships in their social networks, the size and scope of their social networks, their exposure to new information and people and ideas.

The fact that they could share their, the adventures of their lives and even the little things in their lives. Very quickly with a push of a button and they could like and, and, and affirm things that others were doing. That was incredibly exciting to people and changed the way that they reacted to media.

They lived their lives in a variety of ways. But then relatively soon, too, became, began the first backlash wave about what's this doing, particularly to younger children and especially the girls when their messaging that was coming into the world was not necessarily affirming or was showing them parts of life that they struggle to think that they would ever have access to and things like that.

The business model of the companies themselves began to raise questions about, well, how much do they really know about me and how much are they, am I being targeted and manipulated or steered or things like that? Obviously, there were concerns about Harassment, and hate speech, and threats, and all kinds of things like that.

And information warriors themselves taking actions in this. The fourth and final revolution that I've been privileged to watch, and is unfolding in front of our very eyes, and is the central topic of this IGF, is the artificial intelligence.

AI is doing wonders in their life, and they anticipate even more wonders in the future. Their productivity and things like that, but they're also worried about their jobs. And they're worried about bias and discrimination. They're worried about their own autonomy and a way to act. And they're worried about ethical applications.

I heard a number here, I hope someone will fact check me on this if I'm wrong. There are at least 1,300 documented protocols of ethical AI that are now being circulated, and God knows how many more. In more private channels, but it's a sense that there's a a palpable fear that these tools might turn bad, or they might be pulled in bad directions.

So, those are the four revolutions in the backlash, so each of them have affected people's lives, but I also wanted to talk for a minute about other ways that I call them fragmented souls. are affected by these new environments, and again, play through the social, cultural, and legal fragmentations that we're seeing.

Everything that we've studied about those four revolutions shows that different groups have different experiences of the revolutions. And the obvious ones that Pew measured every time something new happened was there are differences by class, differences by gender, differences by age, differences by race and ethnicity, and sometimes pretty significant differences by religious affiliation or non religious affiliation.

There are also differences by psychographics. The way people are affected their relationship to these new tools. First of all, especially when it comes to AI, their awareness. It's an enormous determinant of how they think about it. The less people know, the more scared they are. And, you can see how public education and other just sort of familiarization processes might ease things over time, but that's a big determinant now.

But there are differences among those who are optimists and pessimists, those who trust and don't trust as their starting point with other individuals, extroverts and introverts, and a whole lot of other psychographics. Finally, just to make things confusing from a fragmentation sense, and anybody that's trying to deal with this has to deal with the reality that different people act different ways in these environments.

At one moment, the context is open and affirming, and I want these things in my life, and I would like them available to me. At another moment, I don't want any access to me. I don't want my data being gathered. I don't want to be offered this transactional kind of thing. There are ways in which you can't even predict at the individual level at times whether people are going to like it or not like it, which makes lawmaking hard, which makes rollouts of new products and applications hard and things like that.

And the final one is the sort of big one, which is there's an optimism gap that's at the center of people's thinking about the fragmentation we face. They think each individual thinks I'm doing okay in this environment. They like. These, all of these revolutions for what they bring to their lives but they also think everybody else is messed up by them.

I'm okay, you're not. So they think they're doing fine, but the society is not doing well, and they are, have a split mind thinking about how to reconcile that in, in policy, in culture, in norms, and in technology. Thank you, Sebastian.

Sébastien Bachollet: Thank you very much, Lee. I will give the floor to Jane now, please.

Jane Coffin: Hello for those of you that don't know me, my name is Jane Coffin. I've been rambling around the Internet community and connectivity communities for about 25 years. I've been in government, industry, non profits and start ups.

My last startup was one that I didn't start it up, but it was one of the key people working on the startup to help fund small networks, believe it or not, in the United States, because there are a lot of networks that are not being deployed in the rural, remote, urban, unconnected, and underserved areas.

And it was specifically to take a look at how to fund those networks with creative, innovative funding, aka bringing what people call blended finance and impact investment back to the United States, where it probably should stay for a while because there's a lack of connectivity and things have to change.

And the regulations need to be loosened up a little bit in order for that to happen. During the 25 years that I've been running around I've done a lot of work in what people call the Global South, but the Global South often doesn't call itself that. The common denominators working in those places that are less connected and potentially had fewer regulations and policies.

So helping to bring some policy and regulatory sense in, in some areas and or building regulators actually to help bring in more open connectivity which was always my goal. I was at the Internet Society for 10 years and spent a lot of time working on Internet exchange points and community networks, which I'm going to focus on as some of the core Internet valued entity things that we need related to something called invariance.

And the Internet Society put out a paper called the Internet Invariance. And I want to read the Wikipedia, if I can find it again, definition for you of invariant, which is a constant. It's something that's not changing, and so if some of the key Internet invariants are openness, interoperability, globally connected, and something that I think Vint coined as permissionless innovation.

I'll call it innovation without permission. Those are critical things for building your Internet community and building networks in anywhere. But what we're seeing is some erosion of those key things about the openness, the interoperability, the globally connected part, which is if any endpoint of the, of a network can connect to another endpoint from that global interconnection, this is super important.

Internet exchange points are assigned of some of these invariants because they bring networks together in a very neutral fashion to exchange traffic without a lot of rules. The rules are, of course, based in the protocols that come out of the Internet Engineering Task Force, and some other organizations like the IEEE, if you're doing wireless, sort of Wi-Fi connectivity at the IX.

But those Internet exchange points that we help develop over time. gave people a neutral grounding place to exchange traffic. They were often not regulated and it's been quite something to work over the last 15 to 10 years to make sure that they weren't regulated and to keep them open. We've seen some erosion of that in different countries and I'm not going to name the countries or where some of this is coming from, even in international organizations, where they wanted to standardize the stack of equipment in IXPs, which could have created more challenges and harden the architecture to a degree, that there was less innovation when you're building the Internet exchange points. The other connectivity medium that we were working with so closely and I've been working with in the last couple years as well on a different level on financing them are the community networks.

You can call them municipal networks, open networks, structurally separated networks where there's more networks riding over a network that somebody else runs, the baseline network. But with community networks, you permissionless innovation to just bring in what you'd like from the community out. And if we see more regulation that prohibits community networks, I've been in international meetings where people said I was trying to stand up a terrorist network or, and I thought, wow, okay that's a whole new spin on what I'm trying to do.

But... and it wasn't me. And I should say the expression we used to use was for the community, with the community, by the community. These are organic networks that are built out in places. that have little last mile connectivity to no last mile connectivity or no competitive last mile and middle mile connectivity.

So, I would posit that when we keep seeing spectrum locked in, when we keep hearing people say no, you can't have a different type of network that isn't an incumbent network or designed a certain way. They're locking out innovation, but they're also locking out competition, and they're locking people out of connectivity at a cheaper price.

So, if we're talking about some of the core Internet values of openness, interoperability, global globally connected, and innovation without permission, Internet exchange points, community networks, and working with brilliant technical people in a very innovative way, which is not in a university setting at times.

I've worked with a lot of people in the network operator groups, which I think a lot of people don't know what those are. The NOGs, the network operator groups around the world are some of the best places where you see technical expertise transferred to other people at what I call the local level.

Where you, if you're talking about sustainability and building more Internet infrastructure, it's not just people jetting in. To say you do this way. It's more of a, how do you work with local people to train local people for local connectivity? So I'm going to stop there and just also say that I think Lee had mentioned it, but there are some things that we're seeing with the DSA and with fair share, which by the way I saw so much erosion of this fair share issue.

20 years ago, people were calling the Internet bypass because it was bypassing the traditional telco networks. So for years and years in certain fora, people were locking out the Internet. They didn't want IP based networks in their countries because it was going around the toll booth of the old telco networks.

Now, I'm not anti telco. Full disclosure, I did work for telco years ago, but there's room for everyone in this equation, and I'm going to turn it over back to you, Sébastien.

Sébastien Bachollet: Thank you Very well articulated. I think it will be useful for the follow up of this meeting. Now we have two person online. I would like to be sure that Nii, who will be the next speaker, and Iria, who are available online, and Nii.

Nii Quaynor: Yes, I'm available.

Sébastien Bachollet: Go ahead. Thank you, Nii.

Nii Quaynor: Thanks very much for inviting me to share some views on the topic.

I tend to think Internet means fragments. So, perhaps the fragmentation is elsewhere. I'll be speaking to how AFRINIC, Africa's regional Internet registry what's affected by local legislation in Mauritius, and what impact this could have on regional Internet registries. There's sufficient background information at the AFRINIC.net website on legal cases, but take a look also at the Assisted Review.

I intend to present that though the legislative context is a factor, there were real other challenges, including RIR transfer policies, policy development, process attacks, cyberbullying, legal denial of service. Attacks on the OG, and also on individuals who dare speak.

Misinformation was peddled, even there was cyber squat of the RIR, and so on. Community poisoning, and naturally that generated some internal governance challenges. Surrounding the resources. However, the core the AFRINIC core function of administering resources to operators and end users, according to community developed policies, has so far held up very well.

The good news is that the multi stakeholder approach we practice in our PDP has been resilient and several draft proposals to hijack resources did not reach consensus. Attempts to game the participation in the PDP were also thwarted and a co chair was recalled for the first time. A brief history will put this in context you know, a proposal to establish was made in 97 meetings in 98 in Cotonou and AfNOG 2000, and thus the proposal and AFRINIC itself was established, around 2004 going to 5. It received endorsements and support of several governments and intergovernmental organizations, many African countries, African Union ICT ministers, OIF, Francophonie, E Africa Commission, UNECA, UNICEF Task Force, and many others supported. So, the need to have it established was unquestioned.

The original idea was to establish as an incorporated association, not for gain, in South Africa. But eventually consensus was to develop a decentralized organization with headquarters in Mauritius and other operations in South Africa, Egypt, and Ghana. AFRINIC was blessed with generous financial resources from the government of South Africa and was actually incubated in CSR in Victoria.

And we proceeded to build a headquarters according to the consensus, with additional support from the government of Mauritius. And in Mauritius, we ended up establishing as a private company with membership bylaws. For a decade, the shared objective was clear and was to build the foundations of Internet in Africa.

We lost this shared objective as we went along and interest, personal interest or self interest began. And this began when AFRINIC received the last slash eight of IPv4 in 2011 as per global soft landing policy. The pressures on the common objective started at this time, and transfer policies adopted by other regions questioned service versus property. These policies considered the v4 resources as property to LIRs, but not to the end user on whose behalf LIR justified the resources. Given that people have voluntarily adopted to use the identifiers, we have responsibilities to manage them as public goods, not property. There were discussions on changing scope of RR functions.

Some say RIR are mere bookkeeper versus a registration service. Agreement to be complied, the need basis policy was questioned, out of reaching use of IPs became an issue, meanwhile, of course, board got involved in our case in resource allocation, which was a no. There was misappropriation of legacy v4 by founding staff, which has been addressed and most resources recalled.

The consensus we had weakened and the board got divided resulting in community disagreements. Thank you. We've had three CEOs, 2004, 15, and 19, and none since 2022. In 2021, AFRINIC initiated a Resource Members Assisted Review, according to the RSA. The membership application has compliance requirements, where members shall do specific things, as well as consequences if a member is not compliant.

In the review, some members accepted, some had forged documents. One member who had received more than slash nine in four locations in 2013, 2014, 2015, 2016, refused to comply, saying AFRINIC is a bookkeeper, has no rights, but the member signed the RSA, the member in question also has no ASN and no v6.

AFRINIC followed the RSA and applied the consequences by recalling resources. The member did not seek arbitration, denied AFRINIC rights to assess his compliance, and started litigations. There have been over 55 cases from five companies and directors. A commercial dispute, therefore, had erupted between the member and AFRINIC.

In that year, there were, in 2021, there were Total of 28 cases with member initiating 26 and AFRINIC only 2. 18 of cases were completed with 12 set aside, 4 withdrawn by a member, and 2 not envoyed or by agreement. There were 11 injunctions, 3 state of executions, 4 claims, and 1 contempt. The claims were to amend our register to make the person like a director.

For us, he's not been elected, demanding 1. 8 billion, demanding AFRINIC unused v4 resources, garnishing the company's assets, claiming defamation, and so on. The cases seem frivolous and designed to overwhelm attention, financial resources, and stress governance. This member bullied community members with defamation suits in their countries if they dared mention their name on mailing lists.

However, the substantive case on violations of the RSA by member has not yet been heard. One of other consequent cases damaged board quorum and could not appoint lawyers for court cases to defend AFRINIC nor (?). A recent court order has appointed an official receiver to hold elections to restore governance at AFRINIC.

In summary, someone saw a loophole and decided to harass company, attack the weak part of the IRR system. This started with review of compliance, then we saw abuse of legislation, intimidative attacks in a capital market economy, member created number of confusion, offering alternate IRR based on brokerage and lots of social media misinformation.

On the other hand, AFRINIC is well positioned in the substance, even injunction on it. Transfer policy has completed as not granted. The multi stakeholder in the PDP was strong enough to resist abuse of open participation. We have had support from all RIRs, ICANN, ISOC, governments, members, and community at large.

We just had AIS2023 organized by AFNOG and AFRINIC and hosted by ZADNA in Johannesburg, South Africa. We are organizing community for what to do in the future and we're privileged to receive video message from Vint Cerf and Ambassador Amandeep Gill, U. N. Secretary General, Envoy on Technology. During the opening ceremony, the Deputy Minister of Ministry of Communication and Digital Technology, Filip Mapoulani, did not mince words when he called the heist a neocolonial conquest.

The v4, v6, and ASN resources are for Internet development in Africa, and we, and will not, will be difficult to change the purpose. AFRINIC did not complete the decentralized organization it planned. It could also not get diplomatic protections it had sought. Ironically, AFRINIC went to Mauritius for business stability, for a technology company, but now going through litigation that comes from capital market.

We should not take Internet for granted. And protect it for all. Thank you.

Sébastien Bachollet: Thank you very much, Nii. Very interesting, useful, and I am sure that a lot of people in this room and around the world support you and the people who try to solve the case of AFRINIC, because we all need AFRINIC. And now I will give the floor to I guess it's Iria, can you show us, show on the screen and take the floor, please?

Iria, you need to open your mic because you are muted for the moment, as I can see.

Iria Puyosa: Yeah.

Sébastien Bachollet: Yes. Go ahead then. Thank you. Thank you.

Iria Puyosa: Thank you Sebastian. I kind of go back to what Lee was saying at the beginning, we had a kind of wave of panics of backlash, as he said, and now we are facing all those.

So we are fighting, we are in a moment where we are listening, we are hearing a lot of voices saying we need to regulate, we need to regulate fast, because something sits on serious harm upon us on the Internet. I'm concerned about this, these reactions and this demand for quick response because most of the time these regulations don't over, under pressure are kind ill designed they may break the Internet, and that was what, this is what we are concerned at the moment.

I believe that we need to do more research on the issues before us, define precisely what the problems are, and how the problems we are trying to solve, and not something so big it's impossible to solve. to understand and assess the trade offs between different policies and the way in which there are suitable technical implementations for those policies.

And while we try to regulate too fast, maybe we lost that. In the research I conducted recently in the FLR lab, we were focusing on Knowing the Internet as a whole, but in messaging apps, while we were trying to add in response to the demands of regulating this ad, particularly trying to Introduce content moderation in encrypted and messaged apps.

That was the goal we were listening here in the United States. People concerned about disinformation and foreign influence operations. People concerned about notification of terrorists, violent extremists, species that may drive atrocities, and child sexual abuse material. Most of the claims had the idea of This is happening because these messages that are encrypted, and so

police discontent and so those hands. So this is what is pretty much the, say, a generalization, a simplification of the public conversation, but it's what we're hearing. So, in our research, we find that, well, it's not the case. Most of the content we see, is messaged to us, is positive, is useful for people, for communities, for society, but this thinking about harms is what dominates the public conversation, and will take us, get to the pressure we are seeing over the UK online safety bill and the U. S. keeps online safety at, in which most of the pressure is we need to find a way to moderate content in encrypted apps because everything running there is negative for the society, it's harmful for the society.

What the part of the work we were doing here at the DFRLab was trying to show how the content there was... a variation of content with different purpose, and most of them is was positive, but also how different ways to deal with this harmful content does exist, we don't need to break encryption, we don't need to establish impose content moderations, or be undermining encryption.

So that is the focus of that, that recent research we're doing here. In part our conclusion is one of the issues we sometimes get out the conversation is how these policies for. The flow of data, use of Internet based applications don't consider this is a transnational flow of data.

This is a, it's a territory, it's got affected platform operations. I'm so... Maybe one intended regulation in one country will be affected profoundly, negatively in other countries in which rural love is known as a norm. So, the work we are trying to do is try to find ways for addressing the problems existing in the platform we have.

Breaking the fundamentals of the use, in this case, breaking the encryption you know, we were focusing on messaging ads, but as we know, see, we go after encryption is not needed in, in, in messaging ads, sooner or later. Rather than later, some people are going to say encryption is not needed in the Internet, and we need to get rid of that because there are other harmful contents running in the Internet.

So this is pretty much what we are looking at this moment. I, we see, I see is app perial for the Internet as a whole, when we let this conversation escalate trying to undermine, in this case a Christian in another case could be a another value, another core principle of the integrity of the Internet as, as a, as a space for communications.

Due this shared concern we had in this legal pressure for Quicker regulation, no well defined regulation, no well intended regulation is part of what we are trying to get into the conversation at the moment, trying to find solutions to ensure the respect of human rights, the rule of law. Within the principles of necessity and proportionality, we have attacking the, the aspects where we consider core for the the functioning of Internet based communications and Internet integrity.

Sébastien Bachollet: Thank you very much. Iria, and now last but not least Vint Cerf, please.

Vint Cerf: First of all, thank you for, okay, well, first of all, thank you for inviting me to join you in this session. I think all the preamble just tells you that many of the times when we try to fashion rules To make the system function in a way that's safe and secure, we often end up with unexpected side effects, and some of them you've just heard from me, for example.

I think what's happened over the course of the last decade or so is that the openness of the Internet, which was relatively safe, was a consequence of the people who were using it. In the very early part, the people who used it were the people who were building it. And for the most part, they didn't have any interest in destroying it or abusing it, they just wanted to make it work.

But as time has gone on and as it has become commercially available, then more and more of the world's population have access to this, and their motivations are not exactly the same as what the original engineering teams had in mind. They're interested in using the Internet for... For their own purposes, and there's nothing necessarily apparently wrong with that, I mean, business wants to use the Internet in order to improve business to grow their businesses.

But there are people who are on the Internet who would like to exploit their ability to amplify their voices, to amplify their messages, to deliver malware, to deliver phishing attacks or denial of service attacks, whatever else is motivating them. And governments are have over the past decade or so recognized that these hazards are beginning to arise out of whatever motivations, and so they try to enact laws that will protect people using the Internet. And that's also an understandable motivation. Now, I must admit to you that there are some countries that are more interested in protecting the regime than they are in protecting the the citizens.

Interestingly enough, and difficult the difficulty is that the same mechanisms that might be used to protect the citizens are also... These are useful for iNiibiting legitimate freedom of speech or other kinds of activities that many of us would consider reasonable. And so that we now have a conundrum, which is that in our interest in protecting the safety and security and privacy in the Internet, we may interfere with our ability to hold parties accountable for the bad behaviors that they exhibit on the network.

And that is threading the needle in some sense, perhaps those of us who live in democracies will have to recognize that the authoritarian governments will in fact use the tools that that we would argue are needed to imbue citizens with rights to iNiibit those rights, and I'm not sure that we have the Freedom to iNiibit that or to prevent that from happening.

What that means is that the Internet will not be the same everywhere that we look. You see this happening where Internets get shut down from time to time because the regime believes that it either is necessary to protect the regime or they may even believe that it's necessary to protect citizens from...

Harmful misinformation and disinformation. This leads to a zeal in the legislative corridors to pass laws intended to protect people's interests. And I'll, let me just set aside the laws that are passed to protect the interests of the regimes and just focus on the more democratic environments.

What can happen, however, is that in the intent of those laws. may be laudable, no pun intended but they may also have side effects. So, one possible example is that if if the law requires a 24 hour response to the removal of harmful content, first of all, it may turn out to be literally impossible.

To cite one statistic that you're all familiar with the YouTube application at Google receives somewhere between 400 and 500 hours of video per minute uploaded into the system. I have no idea how many hours of video are exported per minute, by users who are trying to download content. It's not possible for that, that content to be vetted manually.

We don't have enough people to do that, and so we rely on technical means machine learning mechanisms, which we all know are imperfect, and so not only will they not work 100 percent of the time, but they won't catch 100 percent of the problems, and they may catch things that aren't problems, but look like problems, because the algorithms don't know the difference.

Asking a company... The size of Google to do something is one thing, but asking a small and medium sized enterprise to carry out the same kind of filtering may iNiibit that small enterprise from ever existing, let alone growing. So, we have these undesirable side effects of well intended laws.

That may prevent us from building the Internet that we all would like to have. We also, someone mentioned earlier, I guess it was Jane, that there were laws that were passed in the U. S. anyway, the telcos that didn't want competition from community networks. We're able to get laws passed in the states to inhibit the building of community networks on the grounds that if a municipality wanted to build a network, it was the government interfering with freedom competing with private enterprise.

That ignored the fact that a typical arrangement would be that the community would actually have a contract with a private entity to go build the municipal network and operate it, but that was ignored in the zeal to argue the other case. So I'm that

These are not simple problems to solve, and that at the Internet Governance Forum, where we've spent years literally contemplating some of these problems, that we have a kind of responsibility to try to help the legislators and the regulators come to reasonable conclusions. about protecting human interests, while at the same time recognizing that there are responsibilities associated with the use of the Internet.

In a previous session I'm, it came, it occurred to me to remind people about the social contract and Rousseau's observation that along with Safety and security, which people are looking for in their social environment, that they have obligations not to abuse their freedoms. My freedom to punch somebody in the nose stops about one, one centimeter away from Sebastian's nose.

And if I, my, my freedom existed up to that point, but as soon as I complete the action now, I have now violated his rights. So we have still some work to do, and I think especially in the IGF context. We have an obligation to help the legislators and the regulators to find a way forward that preserves as much of the utility and value of the Internet as possible, while at the same time protecting people from harm.

And one particular thing which we valued over time, I think, is anonymous use of the Internet. You shouldn't have to... be known to just do a Google search, for example. However, if you are going to use the Internet for harmful purposes, eventually, I think we would generally agree we would want those parties to be identified.

Well, this gets to the notion that of accountability. Many of the laws that are being passed are attempts by the legislators to articulate how to hold parties accountable for their behavior, whether that's a private sector entity or an individual or a whole country. In order to hold parties accountable, you have to be able to identify them.

So now we have attention. between privacy and the ability to reveal a party in the event that we believe that party is misbehaving. There is currently, as many of an attempt to draft a cybercrime treaty, and there is a considerable amount of debate deciding on what's a cybercrime. In some cases, you could argue that every crime that already exists Can also use a computer to execute the crime, therefore all crimes must be cyber crimes.

That's not a good syllogism, and some of us are arguing that we should be more cautious about the treaty being focused specifically on things that you could not do without the use of a computer and the network. That's still in debate. So we haven't completed that yet. So my bottom line on all of this is that in our attempt to make the Internet a safe and secure environment, we are going to have to accept that some of the principles that we enjoyed in the early days of the Internet may no longer be fully attainable.

And in particular, I would argue that accountability forces us into Making parties identifiable at need. And I will offer just one very weak analogy, which some of you heard before, I suspect. When you get a license plate on the car, it's usually just a random collection of letters and numbers, and it looks like gobbledygook to us.

But there are parties who have the authority to look that license plate up and identify the owner of the car. Which, by the way, may not be the driver of the car, and that's also an important observation. But this piercing of the veil of anonymity or pseudonymity is may turn out to be essential to introducing accountability into the system.

Some of you have also heard my argument that agency is another element of all this. We need to provide agency to individuals, corporations, and even countries. to protect their interests which might mean, for example, the use of end to end cryptography in order to maintain confidentiality. And arguments are often made that end to end cryptography is harmful because it means it's harder for law enforcement to detect that there's misbehavior on the network.

And I draw the line there and argue that end to end cryptography for the protection of confidentiality is extremely important. The idea that you have a backdoor into the cryptographic system almost certainly guarantees eventually that information will be released and then no one will have any confidentiality at all.

Last point. People who are focused on the anonymous use of the Internet may sometimes forget that strong authentication of your identity might turn out to be helpful to you, and that you should be adopting mechanisms that make it hard for other people to pretend to be you. Because if it's too easy for them to do that, they may in fact take actions on your behalf that you didn't authorize.

And so strong authentication might, I hope, become a norm in the system where it's needed in order to make sure that you protect yourself against other people taking actions that you didn't authorize. So, Mr. Chairman, I'll stop there, but I hope this feeds a little bit of the thinking for the debate, which should follow.

Sébastien Bachollet: Thank you very much, Vint. Sébastien Bachollet speaking. Just I would like to pick up one of your points. It's when you remind us that IGF could be useful and the exchange we have here and in the other room. are not just to talk, but also it's to talk, but to exchange between various stakeholders.

And that's an important point here also today. Now I would like to open the floor for questions. You have a mike, in the middle of the room, just queue there and then talk, give comments or questions, and if there is the same online, please do it.

Alejandro Pisanty: Yes Sebastian Alejandro Pisanti here, moderator online.

There's Deborah Allen Rogers hand up as well.

Sébastien Bachollet: Okay, Deborah, go ahead, please. Thank you.

Alejandro Pisanty: Oh, Deborah, you can ask your question.

Sébastien Bachollet: If you can open your mic and eventually your camera, too, will be great. Like that we can see you for the moment your microphone is closed, as I can see.

Vint Cerf: How many engineers does it take to turn on a microphone?

Alejandro Pisanty: Maybe only one, but the system is unresponsive.

Sébastien Bachollet: Okay, maybe okay, maybe Alejandro, you may be willing to start and we will try to solve the problem with Deborah, please. Thank you.

Alejandro Pisanty: Thank you. I'll make a very brief comment right now. As the work of the Dynamic Coalition on Core Internet Values is concerned with the way different Things, and this year it's regulations mostly, may impinge on these core values assuming, of course, that they are mostly the technical principles with which the Internet was built.

And what we see from some of the regulation proposals is that they may actually Do away your damage seriously. Things like the universality of reach of the Internet they may be achieved by reducing interoperability. I'm very concerned for example, this is does not mean not to do it, but find a way to do it with what Vint has said, for example, for stronger authentication or for stronger identification.

We may find ourselves needing to add devices to the system, or some governments or banks or such entities may decide that you need to have an extra device maybe also on their network to do this authentication that open standards like PKI. Will not work. So that's the kind of concern that we have to look into the, to extract a list of these things for now and see how they can be made to work or research over the next months.

These are key points. That we're looking at, but I'll leave the floor to other participants.

Deborah says it's not allowing her to open and I'm already trying to unmute.

Deborah Allen Rogers: Hello. Hello.

Alejandro Pisanty: There you are.

Deborah Allen Rogers: I'm here, but I would like to be on camera, but you all see my face in the picture. So I just want to say hello to everyone.

And thank you very much. I will lower my hand also, and what I wanted to say was a couple of things. I'm from New York City. I live in the Hague. My name is Deborah Allen Rogers, as you see, and I have a digital fluency lab here called find out why. So I wanted to direct my question. Oh, here we go. It looks like I can start my video.

Okay. Hello. Everyone. Okay, so hello from the Hague. I wanted to direct my question at Jane and also at Vint, everyone else who might want to join in, but in particular, the 2 of you. 1 is the father of the Internet. And secondly, as a woman who just gave us a lot of really good intel about NOGs, for example, do either of you or do anyone on the panel spend time working directly with.

I work with Finland and Estonia on e governance. I do some work with them and they've developed these models and they've been putting them in place for a good 20 years for e governance and have answers to many of the questions I see that we struggle with here in Europe and that we struggle with in the United States.

And the last point I'll make is because they stay under the radar screen, oftentimes their designs are overlooked, I've noticed in all the work that I do with various European Internet forums, et cetera. So I was in D. C. this summer and we talked a lot about it at the transatlantic partnership meetings, but I did want to raise it in this venue as well about e governance in Estonia and in Finland and XRoad in particular.

Thank you for taking my question.

Sébastien Bachollet: Thank you, Deborah. Questions in the room? Okay, we can start with a few questions and then but it's... Up to you. If you want, we can start, Deborah, if you want to take the floor and give some answer and then I will ask Vint also and the other participants.

Maarten Botterman: The question does relate to the same thing.

Sébastien Bachollet: Then go ahead.

Maarten Botterman: Do you hear me? Fire the microphone, okay. So, Maarten Botterman and indeed the big thing I'm struggling with is that this Internet needs to be more and more secure, more and more reliable. We can, we should be able to rely on it, and we are working on that. And now, one of the elements is indeed identification.

And would you consider, for instance, anonymity as a core Internet value, or is that something different? How can we get to a kind of standard where... You combine security with anonymity via a kind of trusted service or something? Is that something where we can go and I think it very much compliments to, to Alejandro's concern and what the lady just said identity as used in these governments.

Sébastien Bachollet: Thank you. Vint, go ahead.

Vint Cerf: I actually would like to respond to that specifically. For a long time, I had the view that anonymity was a right that we should have and that you should be able to use the Internet without identifying yourself. What we discovered, at least what I believe we discovered, is that anonymity creates opportunity for really severe and bad behavior.

If people think that there are no consequences for their harmful behaviors on the net, then they will continue to execute those bad behaviors. And so absolute anonymity is, in my view, not necessarily a, should not be a core value. And I, I'm surprised at my change in position, but having seen too much bad behavior that's shielded by anonymity, I now believe that accountability is more important.

That doesn't mean that you have to identify yourself to use all of the Internet's features. That's not what I'm arguing. But I am saying that we should tolerate mechanisms that allow for discovery. And while I say that, I absolutely understand that the, viewing this through the lens of a democratic society versus an authoritarian one, you get very different answers.

From the standpoint of an authoritarian government, the ability to identify parties is harmful to that party's interests. And if we don't allow for that kind of discovery, then all of our interests are harmed by the bad behaviors that are not accountable and therefore difficult to iihibit. You could say, well, can't we inhibit the bad behaviors just by using technology?

Can't we use machine learning to filter all the bad stuff out? And the answer is, as far as we can tell, that doesn't work. Either it doesn't work because it fails to filter, or it filters the wrong thing, and therefore people's rights are harmed because of that. And so this is going to be a relatively imperfect outcome, but I am persuaded at the moment.

That protecting people's interests and protecting people from harm is really important. We can say, though, that there are certain actions that, that where we recognize that anonymity is important because if you're identifiable, then there could be really harmful side effects. Whistleblowing being a good example of that.

But I would argue with you that even in the whistleblowing case, The most traditional means of handling that are that a trusted party receives the blown whistle and may in fact need to know who is blowing the whistle, but is obligated to keep that party's identity anonymous. And that's one of the ways in which you thread the needle between anonymity and identifiability and accountability.

So I'd be very interested, of course, if people have arguments against this proposition that pure anonymity should not be an absolute core value anymore. Thank you. Can I pick up on that, Sebastian?

Sébastien Bachollet: For a second. Go ahead. Yeah. Okay. Go ahead.

Alejandro Pisanty: And, to further the point that was made by Deborah as well how big an architectural change would this vi We have assumed for many years that the only identifier that the Internet gives you is actually, I mean, that's proper from the Internet, is the IP address, and everything else comes from the edge.

So how big of an architectural change would that be? And then, of course, how scalable would that be? The case of Estonia, I think, is very brilliant, but has a limitation of scale in the way you can establish trust within a small community. Society, or going further out. Sorry. So it's just to extend this question. Thank you.

Vint Cerf: Could I respond on the Estonian side? Because the one thing which impresses me about Estonia is that 100 percent of the population is registered for strong authentication. 100%. And they can do that in part because it's a million and a half people. When you get to 300 million or 600 million or 1. 4 billion, it gets harder. India has introduced the Aadhaar system, which is attempting to strongly authenticate parties for their benefit. But everyone sitting in the room and those online can also recognize the potential risk factors of being able to identify people by biological metrics and things like that. And you can see how that can be abused as well.

So, we're, this is a peculiar tension that I think is not 100 percent resolvable, but as I say, I believe that accountability may turn out to be far more important than absolute anonymity.

Sébastien Bachollet: Thank you, Jane, and then I will go to Ghana IGF Remote Hub and then back to Deborah.

Jane, please.

Jane Coffin: I would, I'll be very brief. Debra, we've worked with a variety of governments around the world to work with a variety of governments around the world, so, but if there are some really great practices that we can glean from you, that would be exciting. I wanted to pick up really quickly on a point that Vint made about the IGF having an obligation.

And I think, Vint, that point, one of the points I want to extrapolate from that is to help find a way forward with governments to have inclusive, multi stakeholder inclusion in policymaking and regulation, we start to exclude civil society, the tech, technical community, academia, Yeah. It's very much not going to lead to a better regulatory and policy regime and environment.

And if we don't, the law of unintended consequences may prevail here, where we may force centralization a bit more. Some governments may force centralization in their lawmaking if they aren't including some of the smaller networks, the other instances like Internet Exchange Points and others in the conversation and lockout multi stakeholder inclusion.

So... I just wanted to put that out there before we ended.

Vint Cerf: So Jane this is also supposed to be entertainment for you, so now we'll have this little debate back and forth. You're not saying, I hope, or are you trying to argue that the point I'm making, that absolute anonymity may no longer be a core value in the interests of the people who use the Internet?

Your argument about governments and multi stakeholder

policymaking, I don't understand is an argument against my proposition. It is an argument for the utility of multi-stakeholder perspective in the formulation of policy. And I hope that what I've been saying is not unintentionally misinterpreted.

Jane Coffin: No.

Vint Cerf: As against multi-stakeholders, and I'm a complete fan of that.

Believe that it should be a part of every government's normal practices. So, I see these as two very distinct things, and I hope that's also a correct interpretation of what you were saying. Okay.

Jane Coffin: I think you're helping us point out that the obligation of the IGF is, and it's the uniqueness of the multi stakeholder model in the IGF, to work with governments to make sure that whether it's a discussion on anonymity, or interoperability, and more networks being interconnected openly, is that's more robust policymaking regulation comes through that multi stakeholder discussion.

Vint Cerf: So, in fact, there's a simultaneous obligation, I think, of members of the IGF who care about these things to engage with governments. We need to help the governments appreciate why the IGF is so important to them as they try to formulate policy.

Lee?

Lee Rainie: The striking thing for so many years about tech policy stuff was that it was pre partisan, both here and in Europe in particular. The dynamic we're talking about now, though, has hints and allegations of being swept into partisan polarization. I don't think there's the kind of consensus now that there might have been five or six years ago in the mainstream, in the parties, about whether anonymity is shouldn't be.

Jane Coffin: A core value and you see signs of it in the populist mainstream party dynamics of Europe as well. So this is all, again, to the theme of the day, this is all organic and moving and fluid and it's hard to settle things in that environment.

Sébastien Bachollet: Okay, let's go back to the participants and Ghana, please.

I hope that we can hear you. I know that we can see you, at least in my computer. But go ahead, please, Ghana, and then Deborah, and then I will go to the room and then to the next speakers online. Thank you.

Ghana Remote Hub: Thank you very much. My name is Commuter Joseph, speaking from Pentecost University, Ghana. Whilst we look at the core values of the Internet, I want to ask this question that with the VPN, virtual private networks, people use these networks to bypass restrictions on the Internet, to fraud and infringe on sensitive data of others.

I want to ask what's... so we're looking at, I mean, what can the government do? Or what can we do to help protect the contents of individuals on the Internet? Thank you very much.

Sébastien Bachollet: Thank you again yeah, go ahead Vint.

Vint Cerf: So, I think that I've reached the conclusion that cryptography is our friend in all of this.

For example, there are many places that will insist that information about their citizens must be kept in the geophysical boundary of the country, in the belief or at least they make the argument that somehow that makes it safer. In some cases the motivation behind that is to demand access to the information from the parties who hold the information within the geopolitical boundary of that government.

We hear the term data sovereignty, for example, to argue that data about citizens shouldn't leave the country. I will make the argument that when you insist on that, you actually lose reliability. At Google, for example, we replicate data across our data centers, and we also encrypt it. So that no matter where it goes, when it's addressed, it's encrypted.

When it's transmitted, it's encrypted. We even have a situation or a provision for the possibility that the users hold the keys to the data. And so we don't, no matter where we put it, it is under the control of the users. So my argument here would be to transport, be that transporter data flows and encryption allow you to place data anywhere on the Internet, and protected as long as you manage your keys properly. Now that is a huge challenge because key management is a non trivial exercise, and in fact it's one of the reasons that I did not push public key crypto into the Internet for a while, because while it was being developed, the people who were doing the development were graduate students.

They are not the first category of people that I would rely on for high quality key management. And it's not that they're... Stupid or something, it's just that they get distracted by silly things like PhD dissertations and final exams. So today we have an obligation to help people manage keys and cryptography and to protect their interests and to help them strongly authenticate themselves.

So, I'm, I'm of the view that that's the correct way to handle data protection and not to argue that its physical location is the ideal protection mechanism, but rather cryptography.

Sébastien Bachollet: Thank you, Vint. Deborah, please. Maybe I need to do something. Wait a second. Yeah. Now, I guess...

Deborah Allen Rogers: Try again. There we go.

There I am. Okay. Thank you so much for that. That's a quotable quote. Excellent. Cryptography is our friend, for sure. And to add to the question that was just asked about how do we protect human rights or personal privacy? Cryptography is our friend and thinking about all the different ways in which It can be scaled.

This is what I wanted to say about the point you made about a miilion point 7 users or something like that in Estonia and the cultural sort of, I think the cultural context of that and the idea that now that we're on this online, offline, no line world, scale is such a reference. It's such a, it's changing this concept of what we can do with scale at the push of a button.

And so I speak also to the CEO of XRoad, who's based in Finland, and he talks about a different cultural reference in Finland. One that's a lot more conservative than the one that was in Estonia 20 years building their brand new Internet. Systems and e governance for their banking and their voting and et cetera.

So, I just want to make this point. I was a clothing designer in the 80s and 90s when the entire world existing through a pandemic called AIDS, moving into global manufacturing, all going to China. This is not and I'm in New York at 9, 11, of course, this is not the 1st time I've been through these sorts of.

drastic transitions. As Vint, I mean, I hear George Carlin's voice somewhere in the background of your voice as well, talking about, and for anyone listening, please look up George Carlin. You'll see why. So thank you about the cryptography is our friend comment. And please can, if you all want to speak about, or at least think about this rethinking about this idea of scale and smaller.

Societies that are doing things because test samples are small and it's scaling a functional test sample is what works. And so we have to think about these societies. I'm living in a very highly governed functional society here in the Netherlands now for 3 years. It's different than living in other cultures that are not highly functional at this moment.

I say that in reference to something that you mentioned, Lee. So, I don't want to actually go on record as mentioning which society, but non functional and functional looks very different. And I think the functionality is the point, not the size. Okay, thank you for listening.

Sébastien Bachollet: Thank you, Deborah. We have 12 minutes to go.

We have one question in the room and one speaker in online and Alejandro Pisanty will read some comments online too. Therefore, let's go to the room. Speaker, please.

Roger Dingledine: Hi, Roger. Is this working? Yep. Roger Dingledine, Tor Project. So this word, anonymity, is one that I think about a lot. I actually find the word anonymity to be confusing when people are thinking about it.

I usually use the word communications metadata security, or securing communications metadata. That doesn't trip very well off the tongue, does it? Fair enough, but the reason why I mention this is... Thinking about one of the ways that we've managed to thread the needle to, to manage both of these is looking at it from different layers.

So if you tell people Tor is an anonymity tool, then they say, Oh, well, I guess I can't use Facebook. But it makes perfect sense to log into Facebook over Tor. You're getting to choose. What of your communications metadata you want to reveal. So by default, when you're reaching them, you don't automatically blurt out your identity.

You then get to choose what you tell them. And Facebook doesn't care where you are, they care who you are. And what they mean by that is Facebook level, Facebook application layer of who you are. So you log into Facebook, and from there, at the platform level, there's a completely separate question about anonymity versus accountability.

Do you need your real name? And so on. But the separating those means that at the network layer, you don't automatically identify yourself. Yet, as you say, it might be beneficial in a societal way, or a platform way, or a community way to choose to identify yourself. At a different layer. So that layering mechanism is one, I don't want to say that it solves everything, but it's a, it, I think it helps us get closer to the answer.

Of course we don't want anonymity for everybody all the time no matter what, but we want to give people the choice of who they tell about them.

Vint Cerf: I think that's a really good point, and I appreciate the layering argument, which makes good sense to me. You'll notice that other elements of the Internet design, especially the domain name system, has introduced mechanisms like DOH and DOT and so on in order to protect information at certain layers in the architecture while revealing it at others. And your point about choice is very well taken.

Thank you, Vint. Thank you for your question. Siva please, and then Alejandro, I will give you the floor. I need to...

Okay, go ahead.

Sivasubramanian Muthusamy: Can you hear me? Yes. Okay. Jane was talking about the Internet exchange points and the neutrality, the intended neutrality. As far as I know, some of the Internet exchange points have a commercial business model. And how far are they away from the intended neutrality and also if an Internet exchange point can theoretically be non-neutral.

Can they also become tools in the hands of governments, good and bad governments, to indirectly regulate the Internet or to control the Internet in a certain way? And the positive question on Internet exchange point is there any design to think of an Internet exchange point for interplanetary networks, probably with a peculiar bridge to give a one way connectivity to the global Internet?

Thank you.

Jane Coffin: So, Siva, that's a, I'm going to start with your last point about Internet exchange points and interplanetary, and I can feel Vint, too, right next to me, because I think, are you still the chair of the Interplanetary Working Group, or the?

Vint Cerf: No, I'm not the chairman. I'm a member of the board, but I participate with them, yes.

Jane Coffin: So, you should check out a session on Thursday that Joanna Kulesz will be running with respect to, I think that's data governance, but in any event. There's a paper that Joanna Kulesz and Berna Gur have written and it was funded by the Internet Society Foundation. I'm not this isn't an advertisement for this foundation, even though I worked at ISOC before.

But the paper they put together and another paper put together by the Internet Society by Dan York, who also will be on the panel on Thursday talks about the potential for exchange points in space, with LEOs, low Earth orbiting satellites. Sorry, I should be clearer. It could be a very interesting thing, and then the question is who can participate?

Who's running the network as far as the LEO constellation itself? Is there neutrality if it's only one entity, company that can control all the traffic exchange, or is it only their traffic? It's very complicated right now, with cross border connectivity to potential if you have a transmission going down into one country that beams up to another satellite that's going to beam down into another country, the whole concept of negotiating cross border connectivity issues is complicated wildly. But I'll stop there for a minute, Siva, and then turn to Vint on the interplanetary.

Vint Cerf: Well, let me, just setting aside the spatial notion for a moment. Internet exchange points on the ground are really powerful tools because they allow for connectivity, efficient kinds of connectivity among networks.

But here's a scary thought. Suppose that you're in a regime where the government runs the exchange points and it is required that all traffic between networks go through government operated exchange points, which might lead to surveillance of a kind that you didn't want. That takes us back to cryptography being your friend.

And once again, you can imagine regimes that don't want, encrypted traffic to be running through the exchange points. With regard to putting exchange points or data centers in space, one of the observations I would make is that those typically require maintenance. And so we may have some difficulty getting people up there to do maintenance.

I'm sure everybody in this room does understand and appreciate that the Internet doesn't run itself. There are millions of people who, as a daily job, help keep the Internet functioning. Otherwise it would break pretty quickly and I wish that were not the case. I wish that our designs have been even more robust, but to be quite frank, they require a lot of attention.

Jane Coffin: Yeah. And Siva, to quickly just answer your question, I was referring to the IXs that are the neutral bottom up. You know, not managed by governments, but to Vint's point, there are exchanges where traffic is monitored that's just required by the countries. And so that's something that does happen.

And I'm with Vint on the encryption. The crypto side not cryptocurrency, but encryption. I don't really care about cryptocurrencies right now. I probably should in the future, but... As far as the commercial IXs, that's a different instantiation of exchange point. And they serve a certain purpose, but they're not the bottom up neutral exchanges, that I meant be more clear about..

Sébastien Bachollet: Okay, thank you very much. Now I give the floor to Alejandro. He will give us last feedback on online. And then I will give one minute to each of the five speaker to conclude. Because we will be late in any case. Go ahead, Alejandro, please.

Alejandro Pisanty: Thank you, Sebastian. I'm not going to speak for myself right now. I'm going to read two comments.

One comes from Iria on the chat. She says choosing to identify is different from being forced to reveal your personal identification data in order to access the Internet or an app. And I side totally with that statement.

And the other one comes from the Abuja IGF Remote Hub, in Abuja, Nigeria. I think Nii mentioned that AFRINIC is registered as a private entity in Mauritius. Hasn't this status contributed to the barrage of court cases the regional RIR now faces? While a good number of technical organizations are registered as non profits, shouldn't regional and global technical organizations that govern the Internet be accorded Internet governmental organization status?

Those are the two.

Sébastien Bachollet: Thank you very much. Vint needs to run to another meeting. Therefore may I suggest that if Nii is still online, may want to take one minute the microphone.

Nii Quaynor: The answer to the question of the nature of a registration private company with bylaws, I think the answer is no, because it has really no, no bearing. A commercial dispute. kind of curving between non profit and members, so I don't see that as the direct thing. This is a case of some member who is violating rules, and is refusing to be disciplined, and is beginning to abuse the legal system by generating a barrage of court cases, at the same time trying to break into people's account by offering them money, and so on.

So, it's just a bad case that needs to be dealt with as such because it, it tried to invade the policy process. It failed. It tried to force a co chair got recalled. If you look at all these things, one organization, why generate 20 something cases in a year?

If you really are doing proper business, why would you have so many IPv4 addresses and no network number, no ASN, no v6? So it's obvious what the game is. It's about the interest of hijacking numbers out somewhere else to use. And that one I don't think Africa or the world will want to see that.

Sébastien Bachollet: Thank you, Nii.

We, we have... Less than one minute per person. Iria, please. Two words of conclusion. Sorry for that.

Iria Puyosa: Basically, I think our consensus should be we need technical expertise in every discussion about policy. So, we need to have people who know how to solve the problems, implement the solutions, and we also need the input from civil society, understanding the human rights trade off before moving up to regulation. So, otherwise we may end with bigger problems or a different set of problems that we are trying to solve.

Sébastien Bachollet: Thank you. Lee, please.

Lee Rainie: Just to set the right tone for the ending of this, when we've asked in global surveys, given all the problems that you are now talking about, we're asking questions about in our surveys how hard would it be and how willing would you be to give up the Internet? And there is almost universal, under no circumstances would I give it up. So, we've done a pretty good job by the consumer behavior and consumer sentiment.

Jane Coffin: Thank you. Jane?

Lee Rainie: Don't discount your voice in helping keep the Internet open, globally connected, secure, and trustworthy. Make sure the multi stakeholder model and the IGF continue.

Sébastien Bachollet: Thank you very much. And I want to give the last word to Olivier Crépin-Leblond. If I am here, it's because he's not here. It would have been much better than me to run this meeting, but Olivier, go ahead.

Olivier Crépin-Leblond: The host has unmuted me. Thank you very much, Sebastian. Thank you to everyone who has participated as a panelist and also as a participant in this discussion. The Dynamic Coalition has discussions throughout the year. The work is ongoing. If you're interested in joining the Dynamic Coalition, you can go onto the Internet Governance Forum website, go into intersessional work where the Dynamic Coalitions are all listed, click on the one on core Internet values. And you can join the mailing list. There's no membership fee or anything like that, but we do take our work very seriously. It's extremely important. We will make a report out of this, of today's session. And, of course, it will be taken into account in the IGF messages for Kyoto. So, thanks very much, and thanks, of course to all those people that have helped with organizing this session.

Sébastien Bachollet: Thank you very much, Olivier, Alejandro, and all the speakers. And, meeting is closed now. Bye bye. Bye and thanks everybody.